Автор:
27.10.14 07:20 -

Компания Cisco опубликовала новый значительный релиз Snort 2.9.7.0 , свободной системы обнаружения и предотвращения атак, комбинирующей в себе методы сопоставления по сигнатурам, средства для инспекции протоколов и механизмы для выявления аномалий.

В новой версии добавлена поддержка технологии OpenAppID для разработки межсетевых экранов уровня приложений, позволяющих определять использование протоколов уровня приложений и выявлять в трафике активность конкретных серверных, клиентских и web-приложений. Добавленный в Snort препроцессор OpenAppID позволяет выявлять активность приложения в сети, накапливать статистику об использовании приложений и связанного с ними трафика, блокировать обращение к приложениям на основе правил доступа, создавать расширения для учёта параметров приложений в правилах Snort, сообщать название программы наряду с IPS-событиями в логах и отчётах Snort.

Описания признаков использования протоколов или приложений производится на специальном языке, основанном на Lua. На сайте проекта размещена библиотека , содержащая несколько тысяч готовых детекторов OpenAppID. Кроме правил для выявления отдельных приложений присутствуют детекторы обращений к группам сервисов, например, детекторы для сайтов совместной разработки, web-служб Apple, файлообменников, облачных хранилищ, платформ для блоггеров, интернет-магазинов, платёжных систем и т.д.

В качестве практического применения OpenAppID отмечается реализация и внедрение межсетевых экранов, позволяющих контролировать обращения к приложениям по сети и оперативно блокировать угрозы, связанные с задержкой выпуска для приложений обновлений с устранением уже эксплуатируемых уязвимостей. OpenAppID также может использоваться для построения отчётов об используемых в сети предприятия приложениях, для блокирования нежелательных приложений, для выявления нецелевого использования программ, для раннего выявления попыток взлома приложений, для определения скрытого обращения к web-сервисам и т.п.

Другие улучшения:

- В правила добавлена поддержка опции protected_content, которую можно

использовать для выявления контента по хэшу (например, в правилах вместо открытого текста можно указать его хэш, чтобы скрыть содержимое от администратора сервера);

- В PAF (Protocol Aware Flushing) внесены улучшения для более аккуратного захвата и сохранения почтовых вложений и сообщений, передаваемых с использованием протоколов SMTP, POP и IMAP;
- Добавлена возможность тестирования поведения системы нормализации трафика без непосредственного изменения трафика (при указании опции na_policy_mode:inline-test система только генерирует статистику о ходе нормализации, без её непосредственного применения);
- В препроцессор инспектировния протокола HTTP (HttpInspect) добавлена поддержка распаковки flash-контента, сжатого методами DEFLATE и LZMA, и PDF-контента, сжатого методом DEFLATE, при использовании опций decompress_swf и decompress_pdf. В HttpInspect также добавлен учёт ситуаций одновременной установки нескольких заголовков X-Forwarded-For;
- В препроцессор SSL добавлены дополнительные методы выявления эксплуатации уязвимости Heartbleed ;
- Добавлена новая команда для сброса содержимого пакетов в файл (control socket);

- Препроцессор Stream5 разделён на два отдельных препроцессора Session и Stream6;
- Обеспечена возможность индивидуального включения опций нормализации TCP;
- Увеличена производительности кода пересборки сеансов FTP;
- Улучшена совместимость с платформами OS X 10.9 (Mavericks), OpenBSD, FreeBSD и DragonFlyBSD.

Read more http://www.opennet.ru/opennews/art.shtml?num=40938